Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)
Old: 027557-071
New: 0119-082

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on _____

Signature _____

Typed or printed name _____

Application Number	Filed
09/977,192	October 16, 2001

First Named Inventor
Stefan ANDERSSON

Art Unit	Examiner
2137	WILLIAMS, Jeffery L

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☒ attorney or agent of record.
Registration number 36,075.

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

Kenneth B. Leffler
Signature

Kenneth B. Leffler
Typed or printed name

703-718-8884
Telephone number

July 26, 2006
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required.
Submit multiple forms if more than one signature is required, see below*.

☐ *Total of _____ forms are submitted.

This collection of information is required by 35 U.S.C. 132. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11, 1.14 and 41.6. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Patent
Old Attorney Dkt. No. 027557-071
Attorney Docket No. 0119-082

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	**MAIL STOP AF**
	)	
Stefan ANDERSSON	)	Group Art Unit: 2137
	)	
Application No.: 09/977,192	)	Examiner: WILLIAMS, Jeffery L.
	)	
Filed: October 16, 2001	)	Confirmation No.: 3198
	)	
For: SECURITY SYSTEM	)	

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In conjunction with the Notice of Appeal filed concurrently herewith, reconsideration and allowance of the above-identified application are respectfully requested for at least the following reasons.

The Final Office Action objected to the specification as allegedly failing to provide antecedent basis for terminology introduced into the claims in an Amendment filed on January 5, 2006. Claims 1-19, 28-30, and 32-46 also stand rejected under 35 U.S.C. §112, first paragraph for the same reason. In response, an After-Final Amendment was filed on July 25, 2006 to amend the specification to add the requested antecedent basis. It is assumed that, upon entry of that Amendment, the objection to the specification and the rejection of the claims under Section 112, first paragraph will be withdrawn. These issues are therefore not addressed here.

The Final Office Action variously rejects claims 1-19, 24-30, and 32-50 as allegedly being anticipated by Caputo et al. (U.S. Patent 5,778,071) or obvious over Caputo et al. in combination with one or more other documents. In so doing, the Final Office Action has made at least the following clear errors:

- Asserting that Caputo et al. discloses "establishing a connection with a mobile communications device, wherein said mobile communications device includes a cryptographic module for use in mobile communication (emphasis added);
- Asserting that Caputo et al. discloses "using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said

communications from said computer over said computer network without sending said encrypted communications over said wireless communications network" (emphasis added);

- Asserting that one skilled in the art at the time of Applicants' invention would have been motivated to combine Caputo et al.'s teachings with those of Liebenow et al. (U.S. Patent 6,131,136) to arrive at Applicant's claimed embodiments; and
- Asserting that none of Applicant's claims define a computer having its own cryptographic capabilities separate and apart from those provided by the mobile communications device. (See Final Office Action, Response to Arguments.)

These distinct arguments will be expanded upon below after a brief summary of exemplary embodiments of Applicants' invention.

Embodiments defined by independent claims 1, 19, 24, 28, and 47 are believed to be patentably distinguishable over the prior art of record because they include novel and nonobvious features that enable a single mobile communications device to achieve a unique efficiency in that *a same cryptographic module located in the mobile communications device is used not only to support the device's own communications with a wireless network, but also the cryptography requirements of a local external device, such as a personal computer having its own connection with a network as illustrated in FIG. 1.* In this respect, it is important to understand that the personal computer is not communicating *through* the mobile communications device and the wireless network to get to its own network; its exchanges with the mobile communications device are merely for the purpose of utilizing the cryptographic functions that the mobile communications device can offer.

1. **Caputo et al. does not disclose "establishing a connection with a mobile communications device, wherein said mobile communications device includes a cryptographic module for use in mobile communication"**

The Final Office Action asserts that Caputo et al. disclose this claimed feature at figure 3; column 9, lines 46-60; and column 15, lines 13-39.

Applicant respectfully disagrees because the device disclosed by Caputo et al. is not "for use in mobile communication over a wireless communications network" as variously required by the claims. Instead, the Caputo et al. device requires a wired connection to a network. (See, e.g., Fig. 2 and column 5, lines 62-65: "Further, the connector port 14 is a

modular receptacle which may be directly connected to a data transfer path, such as a telephone system.")

2. **Caputo et al. does not disclose "using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network"**

The Final Office Action asserts that Caputo et al. disclose this feature at figure 3; column 9, lines 46-60; column 15, lines 13-39; column 2, lines 23-27; and column 3, lines 33-38. Applicant respectfully disagrees because, even if the Caputo et al. device were modified to be a mobile communications device communicating with a wireless network, the external device of Caputo et al. would not be capable of "initiating communications from said computer over a computer network ... without sending said encrypted communications over said wireless communications network"; instead, Caputo et al.'s computer is connected to the network *through* the device 10 (see, e.g., Caputo et al.'s figure 2). Moreover, the device of Caputo et al. appears to operate in only one mode, namely, for the benefit of the external device (computer); it sits in-between the computer and the network, passing data from one to the other, and performs cryptographic functions as required by the node that the *computer* is connected to. Consequently, there is no dual mechanism in which the cryptographic module of the mobile communication device is "for use in mobile communication over a wireless communications network" and also for "[acting] as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network."

3. **One skilled in the art at the time of Applicants' invention would not have been motivated to combine Caputo et al.'s teachings with those of Liebenow et al. (U.S. Patent 6,131,136) to arrive at Applicant's claimed embodiments.**

The Final Office Action at least acknowledges that Caputo et al. does not disclose a mobile communication device that is also usable over a wireless communications network, but relies on Liebenow et al. as making up for this deficiency. This reliance is unfounded, however, because Liebenow et al. do not disclose a mobile communication device. Instead,

Liebenow et al. disclose a dual mode modem that automatically switches between a wireless and wire-based communication modes using mode selection circuitry that detects when a wire-based communications network, such as a standard land-line telephone network, is coupled to the modem. Such a device fails to satisfy Applicant's various recitations of "said mobile communications device includ[ing] a cryptographic module for use in mobile communication over a wireless communications network." Rather, Liebenow et al.'s dual mode modem is more of a dumb, slave device that could never be used on its own; it would therefore never require its own cryptographic module for use in mobile communication over a wireless communications network.

Moreover, even if Caputo et al.'s device were modified to include Liebenow et al.'s dual mode capability, the combination would still operate in only one mode, namely, for the benefit of the external device (computer); operating only to passing data between the computer and its network. All cryptographic functions would be performed only as required by the node that the *computer* is connected to, *and would pass through the device to the computer network.* By contrast, embodiments such as those defined by independent claim 28 require that the encrypting device return the encrypted data to the computer for communication over a computer network without sending the encrypted data over the wireless communication network. See also independent claim 44, which defines "a mobile communications device ... comprising a security manager module ... [that] returns the results of the cryptographic function to the computer system ...." Consequently, any combination of Caputo et al. with Liebenow et al. would still lack any dual mechanism in which the cryptographic module of the mobile communication device is "for use in mobile communication over a wireless communications network" and also for "[acting] as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network."

4. **A number of Applicant's claims do define a computer having its own cryptographic capabilities separate and apart from those provided by the mobile communication device, and this is a further distinction over the prior art of record.**

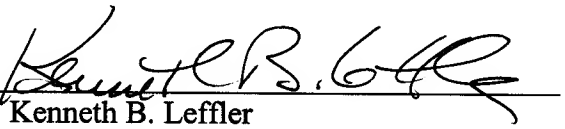
In an earlier Amendment, Applicant had argued this as one of the features that distinguish over Caputo et al. (and the remaining prior art of record), and continues to do so. For example, independent claim 24 defines "*a first part of the required cryptographic functionality being provided in the computer, and a second part of the required cryptographic functionality being provided in the mobile communications device*, ... the computer further comprising an interface device which, on determining that an application needs to use cryptographic functionality, *selects the functionality provided in the computer, or the functionality provided in the mobile communications device*, and sends a command thereto" (emphasis added). See also, independent claim 36, which defines a computer including "a cryptography service provider" separate from the "mobile communication device including a cryptographic module," and claim 42 which defines "the cryptography service provider has some cryptographic functionality, ..."

For at least the foregoing reasons, it is respectfully requested that the various rejections of 1-19, 24-30, and 32-50 as allegedly being either anticipated by Caputo et al. or obvious over Caputo et al. in combination with one or more other documents be reconsidered and withdrawn.

The application is believed to be in condition for allowance. Prompt notice of same is respectfully requested.

Respectfully submitted,
Potomac Patent Group PLLC

Date: July 26, 2006

By: 
Kenneth B. Leffler
Registration No. 36,075

P.O. Box 270
Fredericksburg, Virginia 22404
703-718-8884